AGENDA ITEM 5
AUDIT RESOLUTION STATUS
FINANCIAL STATEMENT AUDIT MANAGEMENT LETTER COMMENTS – PRIOR YEAR
AS OF DECEMBER 31, 2008

Auditor Audit Scope/ (Report Issue Date)	Responsible Division(s)	Finding Number and Description	Current Status
Macias, Gini & O'Connell Report to Management for the Year Ended 06/30/07 (12/14/07)	Investment Office	1. Real estate investment values are derived from independent appraisals when called for by Policy and real estate partnership financial statements. Based on our testing of real estate appraisals, internal controls are not sufficient to ensure that appraised values of real estate investments covered by the CalPERS Investment Policy for Equity Real Estate Appraisal and Valuation are properly recorded by the related partnership. CalPERS established a Performance Monitoring Unit (PMU) in the Investment Office's Administrative Services and Operations Unit. The PMU's responsibility includes selecting appropriate appraisers and finalizing the valuations with the related partnerships, but does not include verifying that appraised values are properly incorporated in the partnership financial records. We recommend that management implement procedures to ensure that appraised values are properly recorded by the related partnership which should include correlation of appraised property to the partnership financial statements. During the fiscal year 2008 audit, PMU developed a process to verify that real estate assets were reasonably reported at appraised values for core real estate. However, we recommend that the same process be completed for non-core real estate properties. PMU should implement procedures to ensure that fair market value of appraised non-core real estate assets are reasonably reported by the partners. In addition, sufficient time should be given for the external auditors to review the work performed and re-perform the procedures on a sample basis.	IN PROGRESS. Investment Office agrees with the current year status. Investment Office will continue to enhance its internal procedures to verify that the appraised value of assets is being reasonably reported by non-core real estate partnerships in their financial statements. In addition, Investment Office will continue its development of a technology-based solution that may assist the external auditor perform their review in a more time-efficient manner.

AGENDA ITEM 5
AUDIT RESOLUTION STATUS
FINANCIAL STATEMENT AUDIT MANAGEMENT LETTER COMMENTS – PRIOR YEAR
AS OF DECEMBER 31, 2008

Auditor Audit Scope/ (Report Issue Date)	Responsible Division(s)	Finding Number and Description	Current Status
Macias, Gini & O'Connell Report to Management for the Year Ended 06/30/07 (12/14/07) *(continued)*	Fiscal Services	2. We noted that real estate investment records utilized by the Performance Monitoring Unit (PMU) do not directly correlate with data maintained by Fiscal Services Division's Real Estate Investment Accounting Unit, which increases the risk of errors in the financial reporting process. We recommend that Fiscal Services Division reconcile quarterly its records in the General Ledger accounts with the records maintained by the PMU of the Investment Office.	COMPLETE. The recommendation has been implemented.
		3. Real estate contribution and distribution accounts capture cash flow transactions relating to real estate investments. Balances in these clearing accounts typically represent timing differences between State Street Bank records and real estate partnership financial statements. During the fiscal year ended June 30, 2007, Fiscal Services had not sufficiently reconciled the balances. As a result, CalPERS recorded an audit reclassification of approximately $628 million to correct the resulting overstatement of real estate income and expenses. We recommend that current accounting practices should be evaluated to ensure that real estate contribution and distribution accounts are sufficiently analyzed and related transactions and balances are properly recorded as part of the ongoing accounting function.	COMPLETE. The recommendation has been implemented.

AGENDA ITEM 5
AUDIT RESOLUTION STATUS
FINANCIAL STATEMENT AUDIT MANAGEMENT LETTER COMMENTS – PRIOR YEAR
AS OF DECEMBER 31, 2008

Auditor Audit Scope/ (Report Issue Date)	Responsible Division(s)	Finding Number and Description	Current Status
Macias, Gini & O'Connell Report to Management for the Year Ended 06/30/07 (12/14/07) *(continued)*	Fiscal Services	4. To obtain the most favorable insurance rates, CalPERS purchases property insurance for all real estate investments. The partnership holding the real estate investment is required to reimburse CalPERS for insurance premium payments. During the fiscal year ending June 30, 2007, insurance premiums paid by CalPERS were not tracked and monitored to ensure the respective partnerships properly reimbursed CalPERS. In addition, we noted several partnerships submitted reimbursements directly to Real Estate Investment Accounting rather than the CalPERS Cashier Unit as required by CalPERS policy. We recommend that management implement procedures to track and monitor the reimbursement of real estate insurance premiums. Outstanding reimbursements should immediately be requested from the respective partnership and payments should be directed to the Cashier Unit.	COMPLETE. The recommendation has been implemented.
		5. Alternative investment values are derived from the related partnership's financial statements as reported by PrivateEdge. During our testing, we noted two instances in which the fair values of alternative investments totaling approximately $80 million had been excluded from the year-end PrivateEdge report and the CalPERS general ledger. Staff did not discover the errors because the values reported by PrivateEdge were not reconciled to the underlying partnership financial statements. We recommend that management implement procedures to ensure that alternative investments are properly valued and reported. Procedures should include reconciling PrivateEdge balances to partnership financial statements as well as evaluating the reasonableness of final valuation adjustments reflected in partnership financial statements.	COMPLETE. The recommendation has been implemented.

AGENDA ITEM 5
AUDIT RESOLUTION STATUS
FINANCIAL STATEMENT AUDIT MANAGEMENT LETTER COMMENTS – PRIOR YEAR
AS OF DECEMBER 31, 2008

Auditor Audit Scope/ (Report Issue Date)	Responsible Division(s)	Finding Number and Description	Current Status
Macias, Gini & O'Connell Report to Management for the Year Ended 06/30/07 (12/14/07) *(continued)*	Fiscal Services	6. CalPERS has elected to unitize certain investment portfolios in order to commingle the investments of the various plans. During our audit we noted several discrepancies between CalPERS' general ledger investment balances and amounts reflected in State Street Bank records. We determined that several transactions relating to the unitization of investment portfolios were erroneously posted to the general ledger, which resulted in two audit adjustments. We also noted inconsistencies in the way in which unitized and non-unitized portfolios are reported in the financial statements. We recommend that current accounting practices be evaluated to ensure that investment activities are consistently and accurately reflected in CalPERS' financial records.	COMPLETE. The recommendation has been implemented.
		7. Retirement benefits are processed in the Retirement Information and Benefits System (RIBS) and the Contribution Reporting System (CRS) subsidiary ledgers, and payments are disbursed by the California State Controller's Office. Fiscal Services reconciles benefit payments recorded in the CalPERS general ledger to the State Controller's Office claims schedule on a monthly basis. However, benefit payments recorded in the general ledger are not periodically reconciled to the underlying RIBS and CRS systems, which is necessary to ensure benefit payments are properly recorded as to period, amount, fund and classification. We recommend that management implement procedures to reconcile benefit payments recorded in the general ledger to amounts reported in the respective subsidiary ledgers.	COMPLETE. The recommendation has been implemented.

AGENDA ITEM 5
AUDIT RESOLUTION STATUS
FINANCIAL STATEMENT AUDIT MANAGEMENT LETTER COMMENTS – PRIOR YEAR
AS OF DECEMBER 31, 2008

Auditor Audit Scope/ (Report Issue Date)	Responsible Division(s)	Finding Number and Description	Current Status
Macias, Gini & O'Connell Report to Management for the Year Ended 06/30/07 (12/14/07) *(continued)*	Health Benefits Branch	8. Blue Cross is the third-party administrator of the self-funded PERSCare and PERSChoice heath plans. Blue Cross reconciles, on a monthly basis, premiums received from the State of California, along with the related enrollment records. During our testing of the PERSCare and PERSChoice premiums for the State's active and retired members, we noted the monthly premium reconciliations were not completed in a timely manner and discrepancies were not properly investigated and resolved. The May premium reconciliation was completed in October and the June reconciliation had not been completed as of the end of October. The Blue Cross premium reconciliations identified the following unresolved discrepancies: ▪ Members were covered under one of the plans, but were not included in participant records provided by the State; therefore, premiums were not paid. ▪ Members were covered and premiums were paid, but members were not included in participant records provided by the State. ▪ Blue Cross records indicate members are covered, but CalPERS records do not indicate coverage and members were not included in participant records. ▪ Payments made by the State differ from the established premiums for selected coverage. We recommend management establish procedures to ensure Blue Cross enrollment records are reconciled to CalPERS and State data in a timely manner. In addition, we strongly recommend that discrepancies are investigated and resolved prior to the next billing cycle or within a reasonable timeframe.	IN PROGRESS. The prior year recommendation was not fully implemented because the June 2008 reconciliation was not completed as of November 2008. The Office of Health Plan Administration (OHPA) and the Office of Employer and Member Health Services (EMHS) continue to emphasize the importance of this reconciliation process. Procedures for this process have been updated. In addition, management has coordinated with Anthem Blue Cross on the timing of the data contained in this report. Moving forward, Anthem Blue Cross will ensure current and accumulative data are contained in this report rather than a 90-day snapshot of the data. Management will continue to focus on ensuring discrepancies are properly investigated and resolved within a reasonable timeframe.

AGENDA ITEM 5
AUDIT RESOLUTION STATUS
FINANCIAL STATEMENT AUDIT MANAGEMENT LETTER COMMENTS – PRIOR YEAR
AS OF DECEMBER 31, 2008

Auditor Audit Scope/ (Report Issue Date)	Responsible Division(s)	Finding Number and Description	Current Status
Macias, Gini & O'Connell Report to Management for the Year Ended 06/30/07 (12/14/07) *(continued)*	Member Services	9. In selecting our sample for testing Legislators' Retirement System (LRS) benefit payments, we noted nine instances in which retiree files did not contain the required documentation. Five member files did not contain the appropriate retirement application, and four files did not contain required proof of age or other documentation. In testing internal controls over the Judges' Retirement System (JRS) benefit payment process, we noted four instances in a sample of 40 of retiree files in which retirement applications could not be located and one instance in which the application was incomplete. Retirement applications include the benefit options selected by retirees as well as other key information used in the calculation of benefits. Without complete retiree files, we were unable to determine whether benefit calculations were correct. In addition, we noted retiree documents for both the LRS and JRS are not imaged in the Document Management System (DMS) in a timely manner, which increases the risk that documents will be misplaced. We recommend the responsible department create a checklist specifying the forms and documents required for processing retirement applications. To ensure the completeness and accuracy of retiree files, staff processing retirement applications should initial each item on the checklist once the documentation has been verified and placed in the file. Supervisory personnel should independently review all retiree files to ensure documentation is complete and the checklist is signed off. In addition, retiree documents should be imaged in DMS in a timely manner, and there should be a centralized filing system for documents which have not been imaged in DMS.	COMPLETE. The recommendation has been implemented.

AGENDA ITEM 5
AUDIT RESOLUTION STATUS
FINANCIAL STATEMENT AUDIT MANAGEMENT LETTER COMMENTS – PRIOR YEAR
AS OF DECEMBER 31, 2008

Auditor Audit Scope/ (Report Issue Date)	Responsible Division(s)	Finding Number and Description	Current Status
Macias, Gini & O'Connell Report to Management for the Year Ended 06/30/07 (12/14/07) *(continued)*	Member Services	10. In testing internal controls over the LRS benefit payment process, we observed that LRS pension benefits are manually calculated and input into the Legislators' Monthly Roll System (LEG) subsidiary system by CalPERS staff. Such manual processes are inherently inefficient and prone to error. We recommend that management consider automating the benefit calculation process.	COMPLETE. The recommendation has been implemented.
	Fiscal Services	11. In testing internal controls over the JRS benefit payment process, we noted two instances in a sample of six months in which the benefit payment claim schedules did not contain the required signature indicating the claim schedule had been reviewed and approved by appropriate supervisory personnel. Fiscal accounting utilizes the claim schedules to record benefit payments in the general ledger system. A signature on the claim schedule indicates that supervisory personnel have reviewed the amounts reported in the claim schedule for accuracy. We recommend that Fiscal Services ensure the claims schedule has been reviewed and signed prior to posting transactions to the general ledger.	COMPLETE. The recommendation has been implemented.

AGENDA ITEM 5
AUDIT RESOLUTION STATUS
FINANCIAL STATEMENT AUDIT MANAGEMENT LETTER COMMENTS – PRIOR YEAR
AS OF DECEMBER 31, 2008

Auditor Audit Scope/ (Report Issue Date)	Responsible Division(s)	Finding Number and Description	Current Status
Macias, Gini & O'Connell Report to Management for the Year Ended 06/30/07 (12/14/07) *(continued)*	Fiscal Services	12. CalPERS adopted the provisions of Governmental Accounting Standards Board (GASB) Statement No. 43, *Financial Reporting for Postemployment Benefit Plans Other Than Pension Plans* (OPEB). The implementation of GASB No. 43 required CalPERS to establish two new funds. The California Employers' Retirement Benefit Trust Fund (CERBTF) was established to account for activities relating to the CalPERS prefunded OPEB plan. The Contingency Reserve Fund agency fund was established to account for activities that were previously reported in the CRF enterprise fund. We experienced delays in the financial reporting and audit process because CRF agency fund transactions could not be easily extracted from the CalPERS general ledger. We recommend that management establish a process to easily identify and record CRF agency fund activities and that management should consider establishing a separate general ledger fund or sub-fund to account for these activities.	COMPLETE. The recommendation has been implemented.
		13. During our testing of administrative expenses, we determined that charges from the Public Employees' Retirement Fund (PERF) to the CRF enterprise fund were not billed in a timely manner. PERF administrative charges for September through December 2006 were not invoiced until February 2007, and charges for February through March 2007 were not invoiced until May 2007. Timely invoicing ensures that revenues and expenses are recorded in the proper period. The prior year recommendation for the CRF was implemented; however, during the current year audit, we noted certain charges were not billed and paid timely in other funds. As such, we recommend that management develop and enforce policies to ensure timely billings for administrative charges for all CalPERS funds.	IN PROGRESS. The prior year recommendation for the CRF was implemented; however, during the current year audit, we noted certain charges were not billed and paid timely in other funds. As such, we recommend that management develop and enforce policies to ensure timely billings for administrative charges for all CalPERS funds. Fiscal Services concurs with the recommendation. Fiscal Services has developed and is following policies and procedures to ensure timely billings for administrative charges between CalPERS funds. CalPERS is current in its billing and recording of administrative expenses to the appropriate CalPERS funds.

AGENDA ITEM 5
AUDIT RESOLUTION STATUS
FINANCIAL STATEMENT AUDIT MANAGEMENT LETTER COMMENTS – PRIOR YEAR
AS OF DECEMBER 31, 2008

Auditor Audit Scope/ (Report Issue Date)	Responsible Division(s)	Finding Number and Description	Current Status
Macias, Gini & O'Connell Report to Management for the Year Ended 06/30/07 (12/14/07) *(continued)*	Information Security Office	14.1 CalPERS policies state that all newly-hired employees will review the CalPERS Information Security Policies and Practices and sign an Information Systems Security and Confidentiality Acknowledgement (ISSACA) form. In addition, all current employees will review and re-sign the form yearly. The form states, among other items, that the employee agrees to abide by CalPERS information systems requirements including the understanding that: ▪ CalPERS information assets and computer resources only for CalPERS approved purposes. ▪ Employees are to access CalPERS systems and networks using only my assigned user identifiers and passwords. ▪ Employees are to notify the CalPERS Information Security Officer immediately of any actual or attempted security violations including unauthorized access; and, theft, destruction, or misuse of systems equipment, software, or data. While CalPERS policy is that all new-hires complete and sign the ISSACA form and current employees re-sign the form yearly, we found that evidence of the signed forms are not always maintained. Our testing of 18 new-hire forms found that 17 percent could not be found. In addition, we tested six current ITSB employees and were only able to find four completed forms. The lack of available signed forms could indicate that either the employee did not complete the review and subsequently sign the form, or that the form had been misplaced. In either case, the evidence of completion of the form is not available putting the agency at increased risk for non-compliance to the information security policies and practices.	IN PROGRESS. The prior year recommendation is in the process of being implemented. Annual web-based training has been instituted to replace the previous ISSACA processes. Our testing in the current year found that approximately 13 percent of our sample of new hires had not completed the on-line training. Additionally, our testing of current ITSB employees found that approximately 14 percent of our sample had not accomplished their yearly refresher training. Current CalPERS standards are not specific as to the timeframe in which training will be completed for either new hires or current employees accomplishing yearly refresher training. The CalPERS Information Security Office (ISOF) should develop standards and procedures to ensure that new-hire web-based training is accomplished within a reasonable timeframe after an employee's start date. Likewise, the timeframe by which current employees should complete their yearly refresher training should be defined. The Information Security Office (ISOF) will establish policies and procedures to ensure that all new employees are identified and awareness training is scheduled for them in a timely manner. The timeframe for current employees to complete the annual training will be determined. *(continued next page)*

AGENDA ITEM 5
AUDIT RESOLUTION STATUS
FINANCIAL STATEMENT AUDIT MANAGEMENT LETTER COMMENTS – PRIOR YEAR
AS OF DECEMBER 31, 2008

Auditor Audit Scope/ (Report Issue Date)	Responsible Division(s)	Finding Number and Description	Current Status
Macias, Gini & O'Connell Report to Management for the Year Ended 06/30/07 (12/14/07) *(continued)*	Information Security Office	14.1 (Continued) CalPERS ISO (Information Security Office) should institute new procedures to ensure that training is provided and new-hires sign the ISSCA form. Periodic internal reviews should be accomplished to ensure this is being done. In addition, procedures should be implemented to ensure that recurring training is accomplished and the recurring ISSCA form is signed and submitted to the Human Resources Department. 14.2 CalPERS has performed an IT risk self-assessment documenting the organizational and management practices, personnel practices, data security practices, information integrity practices, software integrity practices, personal computer security practices, network protection practices and incident response practices. These practice areas were rated with an overall risk score derived from a probability, impact and mitigation control assessment score. The documentation was not readily available to support the effectiveness of the mitigating controls noted in the report. It is these mitigation controls that address the vulnerabilities of the agency and which should be assessed for effectiveness. While an IT risk self-assessment has been performed and is an appropriate step in the development of a comprehensive risk assessment strategy for the agency, the ITSB Technology Services and Support Division should consider the documentation and testing of the mitigation controls noted within the current self-assessment. The effectiveness of the mitigation controls should be established and documented in order to substantiate the mitigation control score used within the risk self-assessment.	The ISOF's goal is to coordinate with the Learning Management System (initially implemented for PSR) to identify staff who have not taken the training. These policies or procedures should be completed by June 30, 2009. COMPLETE. The prior year recommendation has been implemented.

AGENDA ITEM 5
AUDIT RESOLUTION STATUS
FINANCIAL STATEMENT AUDIT MANAGEMENT LETTER COMMENTS – PRIOR YEAR
AS OF DECEMBER 31, 2008

Auditor Audit Scope/ (Report Issue Date)	Responsible Division(s)	Finding Number and Description	Current Status
Macias, Gini & O'Connell Report to Management for the Year Ended 06/30/07 (12/14/07) *(continued)*	Information Technology Services Branch	15.1. Network password configuration standards are not being enforced. The CalPERS Information Security Office has published a formal Information Security Password Practice policy, last updated in 2005. The policy defines a minimum password length and configuration standard. However, the CalPERS network is currently configured with Novell Network managing file and server access and Microsoft Active Directory managing all other network access. This dual separation of network control has resulted in the inability to electronically enforce a password configuration standard. CalPERS is aware of this inability and is currently in the process of moving all of the network control under Microsoft Active Directory. Until then, though, password configuration standards are not being electronically enforced. Until the CalPERS network environment is consolidated within Microsoft Active Directory, the Information Security Office should periodically run a password cracking application to test the complexity of network passwords. Individuals who are found to have used passwords that do not adhere to the CalPERS Password Practice policy should be notified to update their passwords immediately.	IN PROGRESS. The prior year recommendation is in the process of being implemented. The CalPERS project to migrate the Novell Network to the Microsoft Active Directory (AD) environment was completed in June 2008. All network accounts are now managed within Microsoft Active Directory which has the ability to enforce password configuration and expiration standards. However, the Windows Directory and Network Services (WNDS) unit is still in the process of reviewing accounts and ensuring that the password configuration standards apply to all accounts. Currently, the AD environment settings differ from the CalPERS Information Security Identity Authentication Practice in the following areas: <table><tr><td>Configuration</td><td>AD Settings</td><td>IS Identity Authentication Practice</td></tr><tr><td>Password length</td><td>6 characters</td><td>8 characters</td></tr><tr><td>Minimum password age</td><td>0</td><td>1 day</td></tr><tr><td>Password Complexity</td><td>Not required</td><td>Complex passwords required</td></tr></table>

AGENDA ITEM 5
AUDIT RESOLUTION STATUS
FINANCIAL STATEMENT AUDIT MANAGEMENT LETTER COMMENTS – PRIOR YEAR
AS OF DECEMBER 31, 2008

Auditor Audit Scope/ (Report Issue Date)	Responsible Division(s)	Finding Number and Description	Current Status
Macias, Gini & O'Connell Report to Management for the Year Ended 06/30/07 (12/14/07) *(continued)*	Information Technology Services Branch	15.1 *(continued)* 15.2. While assignments to the Active Directory Domain, Schema, and Enterprise Administrative Groups are reviewed by the Windows Directory and Network Services (WNDS) manager to ensure that assignments to the groups are limited and appropriate for the employee's duties, there are no formal guidelines or policies defining who should formally have access to these Admins Groups within Active Directory. Without formal policies defining the positions and duties that would necessitate assignment to these sensitive authorization groups, it is left to personal discretion and institutional knowledge which may be subject to inconsistency depending upon who is ultimately authorizing the access. The CalPERS WNDS manager should develop and implement formal guidelines or policy defining which positions or duties should be allowed access to the Domain, Schema, or	*(continued)* The CalPERS WNDS Unit should continue work on ensuring that the AD environment properly enforces account passwords in accordance with the Information Security Identity Authentication Practice. To implement the recommendation will require customer education and awareness. The level of effort is minimal for WNDS, however, the customer education/awareness needs to be coordinated with the Information Security Office, Enterprise Desktop Customer Support, Customer Support Center and WNDS. Implementation will be in the second quarter of calendar year 2009. IN PROGRESS. The prior year recommendation is in the process of being implemented. The CalPERS WNDS Unit has completed the transition from Novell Network to Microsoft Active Directory and is still in the process of establishing and configuring the Admins groups and developing the guidelines or policy to ensure that only a minimal amount of personnel are allowed access. Implementation is expected to be complete in the second quarter of calendar year 2009.

AGENDA ITEM 5
AUDIT RESOLUTION STATUS
FINANCIAL STATEMENT AUDIT MANAGEMENT LETTER COMMENTS – PRIOR YEAR
AS OF DECEMBER 31, 2008

Auditor Audit Scope/ (Report Issue Date)	Responsible Division(s)	Finding Number and Description	Current Status
Macias, Gini & O'Connell Report to Management for the Year Ended 06/30/07 (12/14/07) *(continued)*	Information Technology Services Branch	15.2 (continued)Enterprise Admins Groups within Microsoft Active Directory. This guideline or policy should ensure that only a minimal amount of personnel are allowed access and that the access is critical to the performance of their duties. 15.3. CalPERS uses an in-house application, Movaris, to manage the workflow used to authorize user account access and authorizations to the various member benefits information systems; CRS, Comet, and RIBS. A review of the process, however, finds that the designated data owners or their formal designees as reported to the Information Security Office, are not required to provide formal authorization prior to a user being allowed access to the application or data. This has the potential to increase the risk associated with the disclosure or integrity of the data as the data owner is not the final approval authority granting access. The CalPERS ITSB should work to ensure that the Movaris application process includes procedures for the formal data owner or the data owner designee to provide approval prior to granting access to an application or data under the responsibility of the data owner. Current user application accounts should also be reviewed by formal data owners to ensure that all accounts currently in use have the proper approvals.	IN PROGRESS. The prior year recommendation is in the process of being implemented. Due to financial considerations, the EIAM project has been postponed indefinitely as of the fourth quarter of calendar year 2008. Security Administration Services (SAS) is now going forward with a transition from Movaris to The Provisioning System (TPS), which was to be an interim replacement until EIAM was fully installed. The plans are now to enhance TPS with the functionality for a data owner approval process workflow. TPS is planned for initial implementation in February 2009, which will include data owner approval workflow for COMET. An enhancement to TPS, scheduled for June 2009, will incorporate data owner approval workflows for RIBS and CRS. As no further development has been done on the Movaris application that would ensure data owner approval prior to granting access to applications or data, the ITSB should continue efforts to implement the TPS and ensure that the automated workflow for data owner approval functions appropriately and that current user accounts are reviewed by formal data owners to ensure that all accounts currently in use have the proper approvals.

AGENDA ITEM 5
AUDIT RESOLUTION STATUS
FINANCIAL STATEMENT AUDIT MANAGEMENT LETTER COMMENTS – PRIOR YEAR
AS OF DECEMBER 31, 2008

Auditor Audit Scope/ (Report Issue Date)	Responsible Division(s)	Finding Number and Description	Current Status
Macias, Gini & O'Connell Report to Management for the Year Ended 06/30/07 (12/14/07) *(continued)*	Information Technology Services Branch	15.4. Shared accounts are being used by the database administrators when accessing the Oracle database or the VSAM file environment. The use of these shared accounts creates a situation wherein actions taken within the database system cannot be tracked back to a specific individual. Inadvertent or malicious activity may not be able to be positively associated with a specific individual essentially eliminating an effective audit trail. CalPERS ITSB should evaluate the use of shared accounts and discontinue their use where it has been determined there is a risk to the database. Database administrator accounts with schema owner access should be controlled with access granted sparingly and only after proper approval has been granted.	IN PROGRESS. The prior year recommendation is in the process of being implemented. The ISOF is in the process of implementing the Guardium SQL Guard appliance to monitor database access and activity. The original implementation date of June 2008 has been pushed back and the test phase of the implementation should now be completed by December 31, 2008. At that time, a decision to implement within the production environment will be made.
	Information Security Office	15.5. Database administrator with accounts to the Oracle database or the VSAM environments may potentially have the capability to alter member information affecting benefits payments. Tests have not been conducted to determine if the database systems have sufficient logging triggers or oversight such as file balancing or reconciliations to verify if unauthorized changes can be detected. The CalPERS Information Security Office should conduct testing to determine if persons with schema owner access to the Oracle database or to the VSAM files can make changes to the database that would affect member benefits without detection.	IN PROGRESS The prior year recommendation is in the process of being implemented. The ISOF is in the process of implementing the Guardium SQL Guard appliance to monitor database access and activity. The original implementation date of June 2008 has been pushed back to the end of fiscal year 2009. To date, no testing has been completed to test for database security assurance. The ISOF has begun the Guardium SQL Guard appliance implementation. The test phase should be completed by December 31, 2008. At that time, a decision to implement into the production environment will be made.